PHAM VAN CHUNG

EGY KLASSZIKUS PROBLÉMA ÁLTALÁNOSITÁSA

ABSTRACT: *(A generalization of a classical problem) The congruence* $x^2 \equiv x \pmod{m^k}$ *was investigated by several authors, the first solution of it was given by M.Tédenat in 1814. In this paper we generalize this problem by solving the congruence* $x^2 \equiv ax \pmod{m^k}$, *where a, m, and k are given natural numbers. We give the number and the explicite form of the solutions and show some properties of them.*

1814-ben az "Annales de Math." c. folyóirat azt a problémát vetette fel, hogy "Melyek azok a természetes számok, amelyeknek négyzete ugyanarra a k-jegyű számra végződik, mint az eredeti szám?" Ezt M. Tédenant [6] oldotta meg először és igazolta, hogy két nem triviális megoldásának összege 10^k+1. Azóta ilyen, illetve hasonló problémával már többen foglalkoztak (lásd [2]). Ehhez a problémához lényegében az $x^2 \equiv x \pmod{10^k}$ kongruenciát kell megoldani.

A problémát a következőképpen általánosíthatjuk: "Melyek azok a természetes számok az m alapu számrendszerben, amelyeknek négyzete ugyanakkora a k-jegyű számra végződik, mint az eredeti szám a-szorosa?" Azaz, keressük az

(1) $$x^2 \equiv ax \pmod{m^k}$$

kongruencia megoldásait.

A kongruencia speciális eseteivel sokan foglalkoztak. Különösen az $m = 10$ esetben értek el sok eredményt.

Érdemes megjegyezni, hogy az $x^2 \equiv x \pmod{m^k}$ megoldásait automorfikus számoknak is nevezték, és ezeket számitógép segitségével ki is számították különböző k értékek mellett. Vernon de Guerre és R.A. Fairbairn [7] -ben kiszámitották az 1000 jegyű automorfikus számokat $m = 6$; 10 és 12. esetben. Itt a szerkesztők megjegyzik, hogy I. Feigberg és T.Moore az 5-re végződő 22.300 jegyű automorfikus számokat is kiszámították.

1972-ben N.P.Callas [1] bizonyította, hogy ha
$x^2 \equiv x \pmod{10^n}$ és

$$y = x^t \sum_{k=0}^{t-1} (-1)^k \binom{t+k-1}{k} \binom{2t-1}{k} x^k ,$$

akkor

$$y^2 \equiv y \pmod{10^{tn}}$$

Általános m esetén az automorfikus számokkal Kiss Péter is foglalkozott, és megadta az automorfikus számok jegyeinek meghatározási módszerét (lásd [4]).

E dolgozatban az (1) kongruencia általános megoldásával foglalkozunk; megadjuk a megoldások számát és a megoldások explicit alakját, valamint a kongruencia numerikus megoldására egy rekurziós eljárást.

G. Vranceanu [8] felvetette azt a kérdést, hogy melyek azok az x természetes számok, amelyekre $x^2 - kx = a \cdot 10^n$, azaz mik az $x^2 \equiv kx \pmod{10^n}$ megoldásai rögzitett k és n mellett. Mi ezen probléma általánositásával foglalkozunk, ahol a,m,k pozitiv egészek. A megoldhatóság szükséges feltétele nyilván az, hogy $x^2 \equiv ax \pmod{m}$ megoldható legyen. Ezért először az utóbbi kongruenciával foglalkozunk.

Megmutatjuk, hogy elég az $(a,m) = 1$ esettel foglalkozni.

1. TÉTEL. Legyenek a és m rögzített pozitív egészek, $m>1$. Az

(2) $$x^2 \equiv ax \pmod{m}$$

kongruencia minden megoldása visszavezethető

(3) $$y^2 \equiv a_0 y \pmod{m_0}$$

alakú kongurenciák megoldására, ahol $(a_0, m_0) = 1$, $a_0 | a_1$ és $m_0 | m$.

BIZONYÍTÁS: Legyen $(a,m) = d$ és tegyük fel, hogy x egy megoldása (2)-nek. Ekkor $a = da_1$, $m = dm_1$ és $(a_1, m_1) = 1$ és (2) alakja

$$x^2 \equiv da_1 x \pmod{dm_1},$$

amiből $d | x^2$. Ha $d | x$, akkor $x = dy$ és (2)-be helyettesítve a

$$d^2 y^2 \equiv da_1 dy \pmod{dm_1}$$

adódik, amiből

$$y^2 \equiv a_1 y \pmod{m_0},$$

ahol $m_0 = \frac{m_1}{(d, m_1)}$, és ez a kívánt (3) alak.

Ha $d \nmid x$, akkor d prímosztóit x is tartalmazza:

$$d = \prod_{i=1}^{S} P_i^{e_i} \quad \text{és} \quad x = \prod_{1}^{S} P_i^{f_i} x' ,$$

ahol $e_i \leq 2 f_i$ $(i = 1,2,\ldots,S)$ de van olyan j, hogy $e_j > f_j$.

Legyen $d_0 = \prod_{1}^{S} P_i^{\left\lfloor \frac{e_i + 1}{2} \right\rfloor}$ és $x = d_0 x'$, ahol $[x]$ az

egész érték függvény. Ezek alapján $d_o^2 = d \prod_1^S P_i^{e_i}$,ahol $e_i=0$ vagy 1 aszerint, hogy e_i páros vagy páratlan. Legyen $d_o^2=dd'$. Igy $d' | d_o$ vagyis $d_o = d'd_1$. Visszahelyettesítve ezeket (2)-be, azt kapjuk hogy

$$dd' x'^2 \equiv dd_o a_1 x' \pmod{d m_2},$$

amiből

$$x'^2 \equiv d_1 a_1 x' \qquad \left(\mod \frac{m_1}{(d', m_1)} \right).$$

Legyen $a_o = d_1 a_1$ és $m_o = \frac{m_1}{(d', m_1)}$; $x' = y$. Ekkor $y^2 \equiv a_o y \pmod{m_o}$, ahol $a_o < a$. Ha $(a_o, m_o) = 1$, akkor a (3) alakot kaptuk. Ha nem, akkor az előbb ismertetett eljárást folytatjuk és $a_o < a$ miatt véges lépésben (3) alakra jutunk, ami tételünket bizonyitja.

Most meghatározzuk az

(4) $$x^2 \equiv ax \pmod{m}; \quad (a,m) = 1$$

kongruencia megoldásait.

2. TÉTEL. (4) kongruencia összes megoldása $x = uy_o$ illetve $x = vz_o$ alakú, ahol $(u,v) = 1$, $u \cdot v = m$, és az y_o, z_o számpár megoldása az $uy+vz = a$ egyenletnek.

BIZONYÍTÁS: Be kell látnunk, hogy minden megoldás a kivánt alaku és viszont.

Tegyük fel először, hogy (4) megoldott és legyen x egy megoldása, azaz $x^2 \equiv ax \pmod{m}$; legyen $(x,m) = u$. Ennélfogva vannak y_o és v egészek, amelyre

$$x = uy_o \quad \text{és} \quad m = u \cdot v \; ; \; (y_o, v) = 1$$

Ezeket (4)-be helyettesítve

$$\left(uy_0\right)^2 \equiv auy_0 \pmod{uv}$$

kongruenciához jutunk, amiből $uy_0^2 \equiv ay_0 \pmod{v}$ és $(y_0,v)=1$ miatt:

$$uy_0 \equiv a \pmod{v}.$$

Innen $(u,v) = 1$, mert másként $(a,m) \neq 1$ lenne, ami lehetetlen a feltétel szerint. Ebből következik, hogy van olyan z egész szám, melyre

$$uy_0 + vz_0 = a,$$

ami bizonyítja a tétel egyik állítását.

Még azt kell igazolni, hogy ha u,v,y_0,z_0 olyan egészek, melyekre $uv = m$, $(u,v) = 1$ és

$$uy_0 + vz_0 = a,$$

akkor $x = uy_0$ és $x = vz_0$ megoldásai (4)-nek. Ez pedig igaz, mert a feltételek miatt az egyenletből például $x = uy_0$ mellett

$$x^2 = (a-vz_0)^2 = a(a-vz_0)-vz_0(a-vz_0) =$$
$$= auy_0-uvy_0z_0 = ax-my_0z_0 \equiv ax \pmod{m}$$

következik.

MEGJEGYZÉSEK: Az előbbi tétel felhasználásával a (4) kongruenciát a következőképpen oldhatjuk meg:

1. Bontsuk fel az m modulust két relatív prím tényező szorzatára, azaz $m = u\cdot v$; $(u,v) = 1$.

2. Oldjuk meg az $uy+vy = a$ egyenletet. Elegendő csak egy (x_0,y_0) megoldást keresni.

3. A (4) kongruencia két megoldása $x \equiv uy_0$ illetve $vy_0 \pmod{m}$.

4. Megkapjuk (4) összes megoldását, ha az előző eljárást megismételjük minden $m = u\cdot v$, $(u,v) = 1$ felbontásnál.

Meg tudjuk adni a megoldások explicit alakját is.

C.P. Popovici [5] bizonyította, hogy $x^2 \equiv x \pmod{10^n}$ kongruencia megoldásai $x_1 \equiv 2^{4\cdot 5^{n-1}}$, $x_2 \equiv 5^{2^{n-1}} \pmod{10^n}$. Azonkivül Goodstein [3]-ben igazolta, hogy ha $m = u\cdot v, (u,v)=1$ és q olyan pozitiv egész szám, hogy $u^q \equiv 1 \pmod{v}$, akkor $x \equiv u^{qv^{k-1}} \pmod{m^k}$ megoldása az $x^2 \equiv x \pmod{m^k}$ kongruenciának.

A mi esetünkben hasonló tétel igazolható.

3. TÉTEL. Legyen $(a,m) = 1$. Ekkor

(5) $$x^2 \equiv ax \pmod{m}$$

kongruencia minden megoldása:

$$x \equiv au^{\varphi(v)} \pmod{m}$$

alakú, ahol $u\cdot v = m$, $(u,v) = 1$ és φ az Euler-függvény.

BIZONYÍTÁS: A 2. Tétel alapján (5) megoldásai $x = uy$ alakuak, ahol $m = uv$, $(u,v) = 1$ és

$$uy \equiv a \pmod{v}.$$

De akkor

$$y = a\cdot u^{\varphi(v)-1} \pmod{v}$$

és igy

$$x \equiv uy \equiv a\cdot u^{\varphi(v)} \bmod v).$$

Szintén a 2. Tételből következik, hogy minden $\left(u, \frac{m}{v}\right) = 1$ feltételt kielégítő u-hoz mod m egyetlen x megoldása tartozik az (5) kongruenciának, továbbá kölönböző u értékekhez inkongruens x-ek tartoznak mod m.

Ezek alapján állapitsuk meg a megoldások számát. Tegyük fel, hogy az m modulusnak r különböző primtényezője van, azaz $m = P_1^{\alpha_1} \ldots P_r^{\alpha_r}$. Mint láttuk, minden $m = u\cdot v$; $(u,v)= 1$ felbontáshoz pontosan 1 megoldás tartozik. Innen következik, hogy (5) -nek annyi különböző megoldása van, ahányféleképpen

m felbontható két relatív prím tényező szorzatára; a tényezők sorrendjét is figyelembe véve. A felbontás a következőképpen történhet: u az m-nek r primtényezője közül tartalmazhat 0,1,2,...,r -et, amíg v rendre: r, r-1, ..., 2, 1, 0 -át. Ezért a megoldások száma

$$\binom{r}{0} + \binom{r}{1} + \ldots + \binom{r}{r} = 2^r .$$

Ezzel bizonyítottuk a következő tételt:

4. TÉTEL. Ha $m = P_1^{\alpha_1} P_2^{\alpha_2} \ldots P_r^{\alpha_r}$ az m szám kanonikus előállítása, akkor az $x^2 \equiv ax \pmod m$ kongruenciának 2^r inkongruens megoldása van, feltéve, hogy $(a,m) = 1$.

Most vizsgáljuk azt az esetet, amikor a modulus m-nek k-adik hatványa, vagyis

(6) $$x^2 \equiv ax \pmod{m^k},$$

ahol $(a,m) = 1$. Mivel m^k-ra ugyanazok a feltételek teljesülnek mint m-re és primtényezők száma is megegyezik, ezért a 2. és 3. Tétel segítségével (6) is megoldható és az inkongruens megoldások száma a 4. Tétel miatt itt is 2^r.

Megkönnyíti azonban (6) numerikus megoldását a következő tétel, ami lényegében a 3. Tétel átfogalmazása.

5. TÉTEL. Ha $(a,m) = 1$, $m = u \cdot v$; $(u,v) = 1$ és

$$y_k \equiv u^{\varphi(v) \cdot v^{k-1}} \pmod{m^k},$$

akkor $x_k \equiv a y_k \pmod{m^k}$ megoldása az (6) kongruenciának.

Lássunk egy példát az 5. Tételre. Legyen például $m = 10$ és $a = 1$, vagyis keressük az $x^2 \equiv x \pmod{10^k}$ kongruencia megoldásait, azaz azokat a k jegyű pozitív egész számokat, melyek négyzetének utolsó k helyen álló számjegyei megegyeznek az eredeti számmal. Például u=5, v=2 esetén

k=1,2,3,4,5 értékekhez tartozó megoldások 5,25,625,0625,90625. Könnyen belátható, hogy ha x_k egy k jegyű megoldás, akkor x_{k+1} az x_k^2 alsó k+1 jegyéből képezett k+1 jegyű szám.

A következőkben a kongruencia megoldásainak összegét vizsgáljuk. Bevezetjük az "alapmegoldás" fogalmát.

Egy kongruencia azon megoldásait, amelyek pozitivak és a modulusnál nem nagyobb számok, alapmegoldásnak nevezzük. Például $x^2 \equiv ax \pmod m$ ilyen megoldásai x=a és x=m , ahol $0 < a < m$.

Ezután bebizonyitjuk a következő tételt, amely megkönnyiti a kongruenciáink numerikus megoldását.

6. TÉTEL. Ha x_1 az $x^2 \equiv ax \pmod{m^k}$ kongruencia egy megoldása, akkor $x_2 = m^k+a-x_1$ is megoldás.

BIZONYÍTÁS: Valóban, ha $x_1^2 \equiv ax_1 \pmod{m^k}$,
akkor

$$x_2^2 = \left(m^k+a-x_1\right)^2 \equiv \left(a-x_1\right)^2 = a(a-x_1)+x_1^2-ax_1 \equiv$$

$$\equiv a\left(m^k+a-x_1\right) = ax_2 \pmod{m^k}$$

ami a tételt bizonyitja.

Megjegyezzük, hogy e tétel speciális esetét már többen bizonyitották a=1 és m=10 esetében először M. Tedénat [6].

A 6. Tételben szereplő megoldáspárok a következő tulajdonságokkal rendelkeznek az $(a,m) = 1$ esetben.

a/ x_1, x_2 legnagyobb közös osztója relativ prim a modulushoz. Ez abból következik, hogy $\left(x_1,x_2\right)=\left(x_1,\ m^k+a-x_1\right)=$

$= \left(x_1,m^k+a\right)$ és $(m,a) = 1$, ezért $\left(\left(x_1,\ x_2\right),\ m\right) = \underline{1}$.

b/ $x_1 \cdot x_2 \equiv 0 \pmod{m^k}$. Ez pedig abból következik, hogy

$x_1 \cdot x_2 = x_1\left(-x_1+m^k+a\right) \equiv ax_1-x_1^2 \equiv 0 \pmod{m^k}$.

Ezen tulajdonságok egy bizonyos megfordítását mutatja a következő tétel.

7. TÉTEL. Legyen x_1, x_2 két megoldása az

$$x^2 \equiv ax \pmod{m^k}, \qquad (m^k,a) = 1$$

kongruenciának. Ha $\left(\left(x_1,x_2\right), m^k\right) = 1$ és $x_1 \cdot x_2 \equiv 0 \pmod{m^k}$ akkor x_1+x_2 is megoldás és

$$x_1 + x_2 \equiv a \pmod{m^k}$$

BIZONYÍTÁS:

$$\left(x_1+x_2\right)^2 = x_1^2+x_2^2+2x_1x_2$$

és a feltételek miatt

$$x_1 \cdot x_2 \equiv 0 \pmod{m^k},$$
$$x_1^2 \equiv ax_1 \pmod{m^k},$$
$$x_2^2 \equiv ax_2 \pmod{m^k},$$

ezért

$$\left(x_1+x_2\right)^2 \equiv a(x_1+x_2) \pmod{m^k}.$$ Tehát x_1+x_2 is megoldás.

De $\left(\left(x_1,x_2\right), m^k\right) = 1$ és $x_1x_2 \equiv 0 \pmod{m^k}$ miatt

$$\left(x_1+x_2\right)\left(x_1+x_2-a\right) \equiv 0 \pmod{m^k}$$

kongruenciából

$$x_1+x_2-a \equiv 0 \pmod{m^k}$$

következik, amiből már adódik a tétel hiányzó állítása.

Az előzőek alapján, mivel a kongruenciánk megoldásai párokba rendezhetők, az inkongruens megoldások összegére könnyen bizonyítható:

8. TÉTEL. Legyen $(a,m) = 1$ és jelöljük S_k -val az

$$x^2 \equiv ax \pmod{m^k}$$

kongruencia inkongruens megoldásainak összegét. Ekkor

$$S_k \equiv a \cdot 2^{r-1} \pmod{m^k},$$

ahol r az m különböző primtényezőinek száma.

BIZONYÍTÁS: A 3. Tétel alapján ha $x_1 \equiv a \cdot u^{\varphi(v)} \pmod{m^k}$ egy megoldás, akkor $x_2 = av^{\varphi(u)}$ is megoldás, ahol $m^k = u \cdot v$; $(u,v) = 1$. De $\left(x_1, x_2\right) = a$ és $(a,m) = 1$. Igy $\left(\left(x_1, x_2\right), m^k\right) = 1$ és $x_1 \cdot x_2 \equiv 0 \pmod{m}$. Ezért a 7. Tétel alapján $x_1 + x_2 \equiv a \pmod{m^k}$. De a 4. Tétel miatt 2^{r-1} ilyen megoldáspár van, ezért a megoldásokra

$$\sum x_i \equiv \sum_{1}^{2^{r-1}} a = 2^{k-1}a \pmod{m^k}.$$

Például: $x^2 \equiv x \pmod{210}$ megoldásainak összege:

$$\sum x_i \equiv 2^{4-1} = 8 \pmod{210}$$

mert $210 = 2 \cdot 3 \cdot 5 \cdot 7$ miatt $r = 4$.

És valóban, számitógép segitségével a következő megoldások adódtak:

$x_1 = 1$	$x_5 = 70$	$x_9 = 106$	$x_{13} = 175$
$x_2 = 15$	$x_6 = 85$	$x_{10} = 120$	$x_{14} = 190$
$x_3 = 21$	$x_7 = 91$	$x_{11} = 126$	$x_{15} = 196$
$x_4 = 36$	$x_8 = 105$	$x_{12} = 144$	$x_{16} = 210$

Ezek összege $\sum x_i = 1688 \equiv 8 \pmod{210}$.

IRODALOM

[1] N.P. Callas, Representations of automorphic numbers, Fibonacci Quart., 10 (1972), 393-396, 402.

[2] L.E. Dickson, History of the theory of numbers, Vol. I, New York, 1952.

[3] R.L. Goodstein, Automorphic number in a general scale, Math. Gaz., 43 (1959), 270-272.

[4] P. Kiss, On one way of making authomorphic numbers, Publ. Math. Debrecen, 22 (1975), 199-203.

[5] C.P. Popovici, Sur une équation arithmétique de D. Pompeiu, Bull. Math. Soc. Sci. Math. R. S. R., 9 (1967), 91-97.

[6] M. Tédenat, Solutions du probléme d' arithmétique, Ann. Math., 5 (1814-15), 309-321.

[7] Vernon de Guerre and R. A. Fairbairn, Automorphic numbers, Journal of Recr. Math., 1 (1968), 173-179.

[8] G. Vranceanu, Asupra unei ecuatii aritmetica, Com. Acad. Rep. Pop. Romane, 3 (1953), 5-8.